



Network Outage Reporting System

User Manual

Version 3

July 28, 2005

Table of Contents

1	Using the System	1
1.1	Accessing the Network Outage Reporting System.....	1
1.2	Security Banner.....	1
1.3	NORS Login	2
1.4	Screen for New Users with New Notifications.....	4
1.5	User Menu Screen.....	6
1.6	Notification Screen	8
1.7	Screen for Selecting the Report to Update or Withdraw	9
1.8	Screen for Updating and Submitting Initial, Draft and Final Reports	10
1.9	Submitting a Final Report.....	11
1.10	Screen for DHS (Retrieval Outage reports).....	13
2	Fields on the Notification Form	15
3	Fields on the Initial and Final Report Forms.....	Error! Bookmark not defined.
4	Descriptions of Root Cause, Direct Cause and Contributing Factors	24

1 Using the System

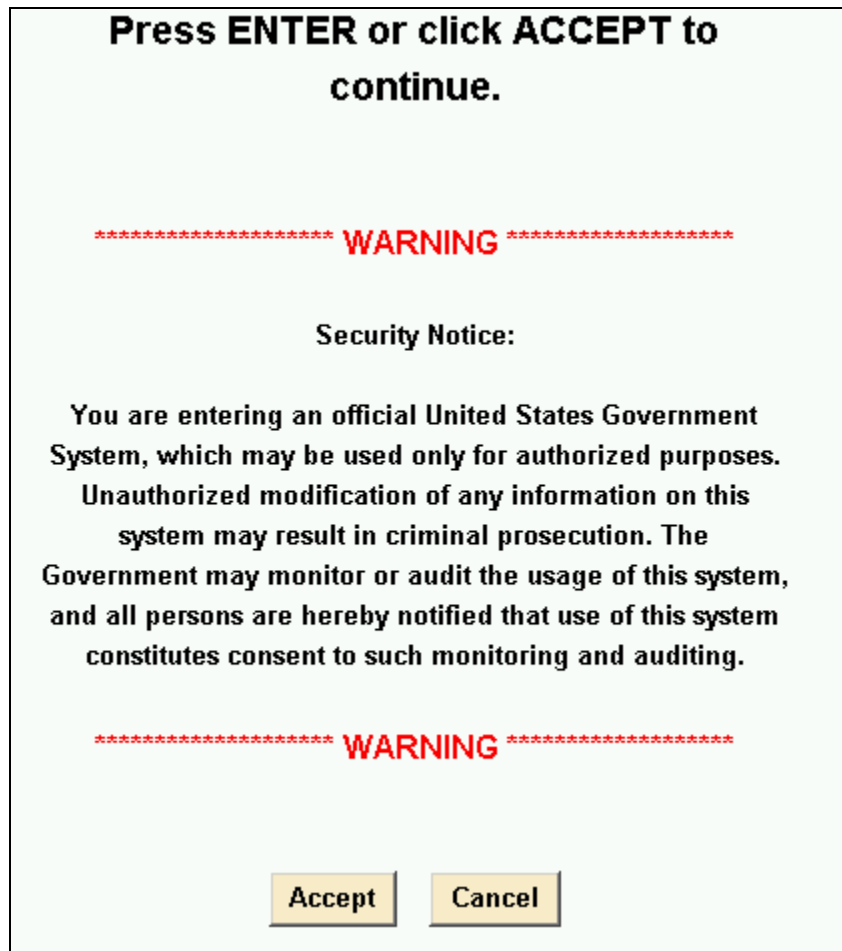
1.1 Accessing the Network Outage Reporting System

The Network Outage Reporting System (NORS) can be accessed by first going to the FCC homepage. The address is www.fcc.gov. Once you are at the FCC homepage, you can find the NORS under the E-Filing menu at the top of the page. Alternately you can go to the Engineering & Technology under Offices on the right side of the home page. The URL is www.fcc.gov/oet/outages. Finally, you may go directly to the NORS using the following URL:

<https://svartifoss2.fcc.gov/prod/oet/ntd/outage/NORS.cfm>

1.2 Security Banner

The following Security Banner will be displayed once the URL for the NORS has been sent:



You will have to acknowledge that you “accept” the conditions stated in the Security Banner.



1.3 NORS Login

There are two main types of users: Department of Homeland Security (DHS) and all others. DHS will be using the “Retrieval” module. All others will be using the “Filing” module. From the “Filing” module, you can view, input, update and withdraw outage reports. All new users should pick the Filing Module. In summary, if you are not from DHS, you will always use the Filing module.

**Welcome to the home page of the
Network Outage Reporting System (NORS)**

*This system is comprised of two separate modules for filing
and retrieving outage reports.*

To continue, choose one of the following:

<p>DHS Retrieval Module *</p>  <p>Retrieve Outage reports - DHS Only</p>	<p>Outage Filing Module **</p>  <p>Report Network Outage</p>
--	--

* For Department of Homeland Security.
** For companies viewing, filing, updating and withdrawing outage reports.

In either case, you will get to a login screen. The Login screen is used to allow outage analysts, outage coordinators and outage inputters to have access to the system. The outage inputters can only report Notifications and update/resubmit/withdraw (and access) only the outages that they personally have already submitted. Outage coordinators will be allowed to modify, resubmit and withdraw any outage except Final Reports from their company.

The outage coordinator has access to all other inputer reports of his company and can also function as an inputer. You will need a User ID and a password. The NORS system User ID and password will be authenticated when you click the Login button on the login screen. The login screen for Filing Outages is:

Network Outage Report System - Filing Login

UserName: (case sensitive)

Password: (case sensitive)

If you don't have username/password, please click [here](#)

If you have forgotten your password, please click [here](#)

If you have questions about this web page, please contact [FCC Outage Help](#).

If you do not already have a User ID and Password, you should click the link marked “If you don’t have username/password, please click [here](#)”. This will send you to the New User screen (given in Section 1.4). Note that if you forget your password, you should click the link marked, “If you have forgotten your password, please click [here](#).” The system will send you to a screen which asks for your UserID and your e-mail address. Your password will be e-mailed to you. If you need help or have questions, you should click the link marked “If you have questions about this web page, please contact [FCC Outage Help](#).”

The login screen for DHS which uses the Retrieving Outages is:

Network Outage Report System - Filing Login

UserName: (case sensitive)

Password: (case sensitive)

If you don't have username/password, please click [here](#)

If you have forgotten your password, please click [here](#)

If you have questions about this web page, please contact [FCC Outage Help](#).

Only DHS users with a valid User ID and Password can log onto the NORS to retrieve outage reports.

If you do not already have a User ID and Password, you should click the link marked “If you don’t have username/password, please click [here](#)”. This will send you to the New User screen (given in Section 1.4). Note that if you forget your password, you should click the link marked, “If you have forgotten your password, please click [here](#).” The system will send you to a screen which asks for your UserID and your e-mail address. Your password will be e-mailed to you. If you need help or have questions, you should click the link marked “If you have questions about this web page, please contact [FCC Outage Help](#).”

1.4 Screen for New Users with New Notifications

If you do not already have UserID, you will be required to identify yourself including providing a valid e-mail address. The system will respond with your User ID and password. You will then be allowed to file Notifications. You will also be able to file and edit Initial and Final Reports for the outages for which you have submitted the original Notification. The screen for New Users is:

New User

Notice: Company ID is needed for users from companies on this list (the default is 11111111). Outage Coordinators set this ID for their company. If you are entering a new company name, you may leave the Company ID blank.

Reporting Company:

New Company (Type in new company name if applicable):

Company ID:

Contact Person:

Phone Number: (###-###-####) Extension:

E-Mail:

If your company has filed an outage report or has an outage coordinator, your company will be listed in the scroll down menu under the Reporting Company. You will have to choose that company and to know the Company ID (or password). The Company ID is controlled by the outage coordinators for your company (if your company has outage coordinator(s)). The default value for it is 11111111. The Company ID is NORS' way to prevent any unauthorized person from saying that he/she is from your company. If your company is not in the scroll down menu, please give the name of your company. You will not have to provide a Company ID in this case.

In all cases you must provide your name, phone number and e-mail address. You will then be sent to the following screen which provides your UserID and password. You can then log onto the NORS and notify the FCC of the outage.

New Reporting Carrier

Your new Username (healyj) and Password (89403301) have been assigned.

1.5 Screen for Forgotten Password Request

This screen allows you to get a new password if you have forgotten your current password. You should click the link marked “If you have forgotten your password, please click [here](#)”.

Network Outage Report System - Password Request

UserName:

E-Mail:

*** Email address must be same as the one in the system.**

NORS will inform you of your new password by e-mail.

1.6 User Main Menu Screen

Those users with valid User IDs and valid passwords who are filing (editing or withdrawing) an outage will go to the User Main Menu Screen upon logging on. Outage inputters and coordinators have slightly different menus. NORS will authenticate your user ID and password and will send you to the correct user menu.

The Main Menu is shown below. The last two selections on the menu are only available to outage coordinators.

Network Outage Report System - Main Menu

- [Find a Report](#) -- To find a report by report number.
- [Report Notification](#) -- To create new outage report.
- [Update/Resubmit/Withdraw Report](#) -- To update/resubmit/withdraw existing outage report.
- [Request to Reopen a Report](#) -- To request to reopen Final Reports.
- [Reports Overdue](#) -- To get the list of overdue reports.
- [Modify Password](#) -- To modify the password.
- [Modify Company ID](#) -- To modify the company id.
- [Deactivate User](#) -- To deactivate user.

This screen provides a menu of items for managing and handling outage reports. This allows an authorized person to find a report by report number, to notify the FCC of a new outage (Notification), or to update, or withdraw a Notification or Initial report, or to file a Final report. There are also the options of requesting that a Final Report be reopened and

obtaining a list of reports where the Finals are overdue or due within the next 5 days. The last two options, only available to outage coordinators, allows them to modify or change the Company ID or to deactivate a user.

If you select **Find a Report**, you will be sent to the Find a Report screen where you can insert the number of the individual report that you want to retrieve. If you are an outage inputter, this allows you to retrieve a report (by report number) that you have personally submitted. If you are an outage coordinator, you can see a report that you or anyone from your company has submitted.. It should be noted that no one from another company can see reports from your company. The only people allowed to view your outage reports are authorized FCC and DHS personnel.

If you are notifying the FCC of a new outage, you should choose **Report Notification**. You will be sent to the Notification Screen. If you want to update or withdraw an Initial report, you should choose **Update/Resubmit/Withdraw Report**. In addition if you want to view your reports, please choose the **Update/Resubmit/Withdraw Report** menu option.

NORS has a provision for the user to ask the FCC to reopen a Final Report by clicking the link marked **Request to Reopen a Report**.. If the FCC agrees to reopen the Final Report, the user can then refile the report.

NORS provides a list of Final Reports that are overdue or due within the next 5 days to encourage the timely filing of reports. This function is available by selecting the **Reports Overdue** function on the menu.

All users should change their password periodically to enhance security of their reporting and viewing of their reports. The menu to change a password is available by selecting **Modify Password**.

The Company ID is a company password maintained by the company's outage coordinators. It is NORS' way of allowing companies with outage coordinators to control who can submit outage reports from their company. Anyone who wants to submit outage reports for a particular company must know the Company ID in order to get a User ID that is assigned to that company. Outage coordinators maintain the Company ID. Outage coordinators can change the Company ID.. This is done under the heading, **Modify Company ID**.

Outage coordinators are allowed to deactivate the privileges of any outage inputters from their company. One coordinator can deactivate another coordinator from their company. This is achieved by selecting **Deactivate User**.

1.7 Find a Report

You can review your company's submitted reports by report number. Coordinators have access to all reports filed by their company. Inputters can only see reports that they have filed. NORS will display the following screen after selecting **Find a Report**.

Network Outage Report System - Search

Outage Number:

The requested report will be displayed.

1.8 Notification Screen

To submit a Notification, you must provide the information on the following screen:

Notification of New Outage Report

If this outage is a national security concern, please call DHS at (703) 607-4950

Name of Reporting Entity (e.g., Company):

Type of Entity Reporting Disruption:

Date of Incident:

Local Time Incident Began (24 hr clock (nnnn)): **Time Zone:**

Reason Reportable:

Effects of the Outage

Number of Potentially Affected

Wireline Users:

Wireless (non-paging) Users:

Paging Users:

Cable Telephony Users:

Satellite Users:

Lost SS7 MTP Messages: **Real-Time:** **Historic:**

Geographic Area Affected

State, Territory, Commonwealth, or the District of Columbia:

City:

Description of Incident

Primary Contact Person:

Phone Number: **Extension:**

E-mail Address:

Details on how to fill out each field are given in Section 2. You have 60 minutes to fill in the form. The timer shows in the status bar at the bottom left of the screen. No information will be stored unless you hit the “Submit” button. Once you hit this button, the Notification has been filed unless an error message appears telling you that one or more of the fields has been filled out incorrectly. You can then correct the data and resubmit. NORS will provide the report number for future reference after a successful filing. Note that the name of your company can not be changed. A copy of the completed Notification can be saved in Excel or you can print the report using the File>Print commands.

When you are ready to submit an Initial or file a Final Report, you will have to logon to NORS and access the correct Notification. To do this, select **Modify/Resubmit/Withdraw a Report.**

1.9 Screen for Selecting the Report to Update or Withdraw

There are four types of reports: Notifications, Initial Reports, Final Reports, and Drafts. A Draft is an informal copy of a report that the system keeps.

The system allows you to choose outages listed by date and by report type. For example, you can list only your Notifications during the month of September. NORS lets you list reports of all types by picking “All”. In addition, NORS also lets you list all “Active” reports – these are reports that are updatable. This includes Notifications, Initial Reports, and Draft Reports, but excludes Finals and Withdrawn reports.

If you select any report, excluding Final Reports, you will be able to update, and resubmit or withdraw it. In particular, if you choose a Notification, you will be able to modify it and then submit it only as an Initial, Final, or Withdrawn Report. Withdrawn reports are not deleted from the database – they are simply marked as withdrawn.

The following screen will come up for users who select Update/Resubmit/Withdraw a Report. This screen is for anyone updating a Notification to an Initial, Draft, Final or Withdrawn Report or updating an Initial or Draft Report. The system allows users to save Drafts of reports and to revise Initial Reports, but Final Reports are formally filed reports.

No government agencies outside the FCC (including DHS) can see Drafts.

Network Outage Report System - List

Notice:
 1. "Active" report type has been added.
 2. Retains the changed from/to dates after returning from "Display", "Update" and "Withdraw".

From: To: Report Type:

Reference Number	Report Type	Company Name	Notification Date/Time	Updated Date/Time			
04-00000860	Notification	TEST COMPANY	12/21/2004 10:09	N/A	<input type="button" value="DISPLAY"/>	<input type="button" value="UPDATE"/>	<input type="button" value="WITHDRAW"/>
04-00000859	Initial	TEST COMPANY	12/21/2004 10:08	12/21/2004 10:10	<input type="button" value="DISPLAY"/>	<input type="button" value="UPDATE"/>	<input type="button" value="WITHDRAW"/>

You will be able to create a list all the outages that you are able to view, update, and withdraw. Outage inputters will be allowed to view, update or withdraw any Notifications, Drafts or Initial reports that they personally have submitted. Outage coordinators can view, update or withdraw any Notifications, Drafts or Initial Reports from their company. No one can update a Final report. Users may request the FCC reopen a Final Report..

1.10 Screen for Updating Notifications, Initial Reports and Drafts, and Filing Final Reports

The following screen will come up once you have selected a report to update. The screen will present the most recent version of the report. **This form must be filled out in 60 minutes and submitted.** This means that the text for most of the text fields should be already prepared and cut and pasted into the form. If you do not hit the "Submit" button within 60 minutes, all your changes will be lost and you will have to start over (logon to NORS again). The system gives a 10 minute warning.

The top of this form is shown below. In section 3, there is a detailed explanation of how to fill out each of the fields.

Outage Report

Report Number: 05-20753626

Notification Date-Time: 07/26/2005 14:53

Report Type:	Initial Report		
Name of Reporting Entity (e.g., Company):	TEST COMPANY 1		
Type of Entity Reporting Disruption:	Cable telephony provider		
Date of Incident:	07/26/2005		
Local Time Incident Began (24 hr clock (nnnn)):	0800	Time Zone:	Atlantic
Reason Reportable:	Wireline - 900,000 user-minutes		
Outage Duration:	0 Hrs	0 Min	
Explanation of Outage Duration (for incidents with partial restoration times)			
<div style="border: 1px solid gray; height: 50px;"></div>			

1.11 Filing a Final Report

If the report type is a Final Report and you hit the submit button, the following screen will come up:

Security Notice:

I am authorized by the communications provider to legally bind the provider to the truth, completeness, and accuracy of the information contained in this report. I attest that I have read the report prior to submitting it and on oath depose and state that the information contained therein is true, correct, and accurate to the best of my knowledge and belief, and that the communications provider on oath deposes and states that this information is true, complete, and accurate.

To actually file the Final Report, you will accept the above statement that states that you are authorized to file the report and that your company deposes and states that the information is true, complete, and accurate.

1.12 Reports Overdue

NORS will provide information on reports overdue and reports due in 5 days by selecting Reports Overdue.

Overdue Reports As of 06/07/2005					
Overdue Initial Reports					
Reference Number	Company	Incident Date - Time	POC	Phone Number	Email
05-12439966	TEST COMPANY 1	05/04/2005 - 0300	John Healy	202-418-2448	john.healy@fcc.gov
05-12439966	TEST COMPANY 1	05/04/2005 - 0300	John Healy	202-418-2448	john.healy@fcc.gov
05-13737922	TEST COMPANY 1	05/17/2005 - 0400	John Healy	202-418-2448	john.healy@fcc.gov
05-13737922	TEST COMPANY 1	05/17/2005 - 0400	John Healy	202-418-2448	john.healy@fcc.gov
05-14346766	TEST COMPANY 1	05/23/2005 - 0400	John Healy	202-418-2448	john.healy@fcc.gov
05-15343733	TEST COMPANY 1	06/02/2005 - 0400	John Healy	202-418-2448	john.healy@fcc.gov

Overdue Final Reports					
Reference Number	Company	Incident Date - Time	POC	Phone Number	Email
05-12439966	TEST COMPANY 1	05/04/2005 - 0300	John Healy	202-418-2448	john.healy@fcc.gov
05-12439966	TEST COMPANY 1	05/04/2005 - 0300	John Healy	202-418-2448	john.healy@fcc.gov

Final Reports Due Within 5-Days					
Reference Number	Company	Incident Date - Time	POC	Phone Number	Email
<input type="button" value="SAVE AS EXCEL"/>					

1.13 Modify Password

This screen allows you to modify or change your password.

Network Outage - Modify Password	
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Re-type New Password:	<input type="text"/>
<input type="button" value="SUBMIT"/>	<input type="button" value="CLEAR"/>

NORS will confirm your change of password.



Use your selected password for future outage reporting.

1.14 Modify Company ID

This screen allows outage coordinators to modify or change their Company's ID.

A screenshot of a web form titled "Network Outage - Modify Company ID". The form contains three input fields: "Old Company ID:", "New Company ID:", and "Re-type New Company ID:". Below the input fields are two yellow buttons: "SUBMIT" and "CLEAR".

NORS will confirm the change of Company ID.

1.15 Deactivate User

Outage coordinators can stop the access to NORS of their company's outage inputters and other outage coordinators from their company by using this menu.

A screenshot of a web form titled "Network Outage - Modify User". The form contains five input fields: "UserName:" (a dropdown menu showing "john.healy"), "Name:" (text input "John Healy"), "Phone Number:" (text input "202-418-2448"), "Extension:" (text input), and "E-Mail:" (text input "john.healy@fcc.gov"). Below the input fields are two yellow buttons: "DEACTIVATE" and "CLEAR".

1.16 Screen for DHS (Retrieval Outage Reports)

The NORS has a module so that DHS can view outages. If you have chosen the retrieval module and successfully logged onto NORS (see Section 1.3) thus gaining access to the

retrieval module, you may select an outage to view. DHS can not change any contents of any report.

Network Outage Report System - List									
From:		12	21	2004	To:	12	21	2004	RETRIEVE
Reference Number	Report Type	Company Name	Notification Date/Time	Updated Date/Time					
04-00000883	Notification	SBC	12/21/2004 13:14	N/A	DISPLAY				
04-00000882	Notification	SBC	12/21/2004 13:14	N/A	DISPLAY				
04-00000881	Notification	SBC	12/21/2004 13:14	N/A	DISPLAY				
04-00000880	Notification	SBC	12/21/2004 13:11	N/A	DISPLAY				
04-00000879	Notification	SBC	12/21/2004 13:09	N/A	DISPLAY				

2 Fields on the Notification Form

Name of Reporting Entity – This lists the name of the company filing the outage report. This field is automatically filled out. It is the name of the company that the outage inputter used when he/she applied for a UserID. Outage reports must be filed with the FCC by any cable communications provider, wireless service provider, satellite operator, SS7 provider, wireline communications provider, E911 service provider, or facility owner that experiences an outage meeting the reporting thresholds as defined in Part 4 of the Commission's Rules and Regulations on any facilities which it owns, operates or leases.

Type of Entity Reporting Disruption – Pick from the scroll down menu the type entity your company is relative to the incident being reported. The choices are:

- Wireline carrier
- Wireless carrier
- Cable telephony provider
- Paging provider
- Satellite provider
- SS7 network provider
- E911 service provider
- Facility owner or operator

If a company is a carrier like BellSouth which provides SS7 service, E911 service and is a facility owner, that carrier should identify itself as a wireline carrier. The designation SS7 network provider is for companies that only provide SS7 service. Similarly the designation E911 service provider is for companies that only provide some portion of E911 service. The designation Facility Owner is for companies that are not carriers but own, operate and lease facilities for use in telecommunications. If a company is a carrier like Sprint which provides both wireline and wireless service, choose the designation which most closely relates to the incident being reported.

Date of Incident - Provide the month, day and year at the commencement of the outage. The expected format is mm/dd/yyyy. To make a change from today's date, automatically inserted by NORS, delete the entire date.

Local Time Incident Began (24 hr clock) - Provide the local time at the location of the, outage (not the reporting location) of commencement of the outage (24-hour clock). That is, for 1:00 PM, you should use 1300. The format should be XXXX; that is, do not use a colon (this number should be between 0 and 2359). In most cases both the physical location of the outage and the majority of the effects are in the same time zone. However, some outages have wide-ranging impacts which may not be at the physical location of the outage, such as a cut undersea cable. In that case, please provide the time at the end of the undersea cable closest to the US or the local time of the physical outage. You should include more detailed explanations in the Initial or Final Report.

Time Zone – Pick from the scroll down menu one of the following:

Atlantic
Eastern
Central
Mountain
Pacific
Alaskan
Hawaii-Aleutian
Guam
Other

Puerto Rico is in the Atlantic Time zone. Other should be used for some place like American Samoa.

Number of Potentially Affected

Wireline Users – Provide the sum of the number of assigned telephone numbers potentially affected by the outage and the number of administrative numbers potentially affected. If this outage did not affect wireline users, please leave this blank.

“Assigned numbers” are defined as the telephone numbers working in the Public Switched Telephone Network under an agreement such as a contract or tariff at the request of specific end users or customers for their use and include DID numbers. This excludes numbers that are not yet working but have a service order pending.

“Administrative numbers” are defined as the telephone numbers used by communications providers to perform internal administrative or operational functions necessary to maintain reasonable quality of service standards.

Wireless Users – Provide the number of potentially affected wireless users. In determining the number of users potentially affected by a failure of a switch, a concentration ratio of 8 shall be applied. If this outage did not affect wireless users, please leave this blank.

Paging Users - Provide the number of assigned telephone numbers for those paging networks in which each individual user is assigned a telephone number. If this outage did not affect paging users, please leave this blank.

“Assigned numbers” are defined as the telephone numbers working in the Public Switched Telephone Network under an agreement such as a contract or tariff at the request of specific end users or customers for their use. This excludes numbers that are not yet working but have a service order pending.

Cable Telephony Users - Provide the number of assigned telephone numbers. If this outage did not affect cable telephony users, please leave this blank.

“Assigned numbers” are defined as the telephone numbers working in the Public Switched Telephone Network under an agreement such as a contract or tariff at the request of specific end users or customers for their use and include DID numbers. This excludes numbers that are not yet working but have a service order pending.

Satellite Users – Provide the number of satellite users affected (if known)

Number Affected

Blocked Calls – Provide the number of blocked calls. If no calls were blocked, please leave the field blank or put 0 down. If blocked call information is available in only one direction for interoffice facilities which handle traffic in both directions, the total number of blocked calls shall be estimated as twice the number of blocked calls determined for the available direction.

If real time information is not available, providers may provide data for the same day(s) of the week and the same time(s) of day as the outage, covering a time interval not older than 90 days preceding the onset of the outage in an effort to estimate blocked calls. In this case, the number of blocked calls reported should be 3 times the historic carried load.

If, for whatever reason, real-time and historic carried call load data are unavailable to the provider, even after a detailed investigation, the provider must estimate the carried call load based on data obtained in the time interval between the repair of the outage and the due date for the Final Report; this data must cover the same day of the week, the same time of day, and the same duration as the outage. Justification that such data accurately estimates the traffic that would have been carried at the time of the outage must be available on request. In this case, the estimate of the number of blocked calls reported should be 3 times carried load. The number of blocked calls, if known, must be filled out even if it is not the trigger for an outage being reportable.

Real-Time, Historic Check Box - Check off whether the number of Blocked Calls came from real-time data or was based on historic carried loads the same day(s) of the week and the same time(s) of day as the outage.

DS3s – Provide the number of previously operating DS3s that were affected by the outage regardless of the services carried on the DS3s or the utilization of the DS3s. If service was provided over an OC3c or OC12c assume that all of the capacity was working and report 3 DS3s for an OC3c or 12 DS3s for an OC12c etc.

Lost SS7 MTP Messages - In cases of an SS7 outage and where an SS7 provider cannot directly estimate the number of blocked calls, provide the number of real-time lost SS7 MTP messages or the number of SS7 MTP messages carried on a historical basis. Historic carried SS7 MTP messages should be for the same day(s) of the week and the same time(s) of day as the outage. The information should not be older than 90 days preceding the onset of the outage. If the outage does not affect an SS7 network, please leave this field blank..

Geographic Area Affected

State – Choose the (primary) state from the scroll down menu affected by the outage. All 50 states along with the District of Columbia and Puerto Rico are listed. Outages affecting major parts of more than one state should be listed as multi-state. If an outage occurred outside the fifty states, the District of Columbia, or Puerto Rico, please choose “Outside the 50 States”.

City – Provide the (primary) city affected.

Description of Incident - Provide a narrative which describes the sequence of events leading up to the incident, the steps taken to try and resolve the incident once it had occurred, and the action(s) which finally brought resolution to the incident. This is for the reader to better understand what has happened. Include any factors which may have contributed to the duration of the incident, "quick fix" actions which may have resolved the immediate problem but were not the final, long-term solution, and any other contributing factors. At the Notification stage, it is anticipated that many of the details will not be known.

Primary Contact Person – Provide the full name of the primary contact person

Phone Number – Provide the phone number of the primary contact person in the format NXX_NXX_XXXX. That is, 201-444-5656 would mean that the area code or NPA is 201, the central office code is 444, and the line number is 5656.

Extension – Provide the extension number, if used, in format XXXX.

E-mail Address – Provide the e-mail address of the primary contact person.

3 Fields on the Initial, Draft, and Final Report Forms

Note that all of the data previously filled in are carried forward when updating a report. All fields can be changed to reflect new information except the Report Number, Name of Reporting Entity, Type of Entity, and the Date-Time of the previous submission.

Report Number – List the unique identifying number for the report. This field is automatically filled in from the Notification.

Date-Time – Self-explanatory. This field is automatically filled in based on the time of the previous submission for the same report number.

Report Type – Choose the type of report: Initial, Draft or Final. Initial Reports are due within 3 days of the outage. Final Reports are due within 30 days of the outage from when the outage started. The Initial Report shall contain all pertinent information immediately available on the outage and shall be submitted in good faith. The Final Report shall contain all pertinent information on the outage in greater detail, including any information that was not contained in, or that has changed from that provided in, the Initial Report.

Name of Reporting Entity – Lists the name of the company filing the outage report which is the same used by the outage inputter when he/she applied for a UserID. This field is automatically filled in. Outage reports must be filed with the FCC by any cable communications provider, wireless service provider, satellite operator, SS7 provider, wireline communications provider, E911 service provider, or facility owner and on any facilities which it owns, operates or leases that experiences an outage that meets the reporting thresholds as defined in Part 4 of the Commission's Rules and Regulations.

Type of Entity Reporting Disruption – Lists the type entity your company is. This entry is automatically filled with the information taken from the Notification. The possible entries were:

- Wireline carrier
- Wireless carrier
- Cable telephony provider
- Paging provider
- Satellite provider
- SS7 network provider
- E911 service provider
- Facility owner or operator

Date of Incident - Provide the month, day and year at the commencement of the outage. The expected format is mm/dd/yyyy.

Local Time Incident Began (24 hr clock) - Provide the local time at the location of the, outage (not the reporting location) of commencement of the outage (24-hour clock). That is, for 1:00 PM, you should use 1300. The format should be nnnn; that is, do not use a colon (this number should be between 0000 and 2359). In most cases both the physical location of the outage and the majority of the effects are in the same time zone. However, some outages have wide-ranging impacts which may not be at the physical location of the outage, such as a cut undersea cable. In that case, please provide the time at the end of the undersea cable closest to the US or the local time of the physical outage.

Time Zone – Pick from the scroll down menu one of the following:

Atlantic
Eastern
Central
Mountain
Pacific
Alaskan
Hawaii-Aleutian
Guam
Other

Puerto Rico is in the Atlantic Time zone. Other should be used for some place like American Samoa.

Outage Duration - Provide the total elapsed time (hours and minutes) from the commencement of the outage as provided in the preceding data fields until restoration of full service. Full service restoration includes the restoration of all services to all customers impacted by the outage even if the restoral is over temporary facilities. If the customers' locations are destroyed such as by a hurricane, flood, tornado, or wildfire the duration continues until the reporting carrier is capable of again providing service to those locations. If an outage is ongoing at the time the Final Report is filed, report the outage duration as the total time between the commencement of the outage and the time the Final Report is filed..

Explanation of Outage Duration (for incidents with partial restoration times) – Describe the stages of restoration if different blocks of users were restored at different times. Often times significant blocks of users may be restored to service prior to full restoration of service. If this is the case, provide information on the number of users in each block restored to service and the elapsed time to partial so that an accurate assessment of the outage impact may be made. In addition, it is important to report when some services, e.g., E911, are restored if different than other services.

Inside Building Indicator – Indicate whether the outage occurred inside a building owned, leased, or otherwise controlled by the reporting entity. A building is a structure that is temperature controlled.

Effects of the Outage - Services Affected

Cable Telephony – Check the box if cable telephony users were affected.

Wireless (other than paging) - Check the box if wireless users were affected.

E911 - Check the box if E911 service or some aspect of E911 service was affected.

Paging - Check the box if paging users were affected by the outage.

Satellite - Check the box if satellite facilities were affected by the outage.

Signaling (SS7) - Check the box if SS7 service was affected by the outage.

Wireline - Check the box if wireline users were affected by the outage. This includes whether intraLATA or interLATA service was affected.

Special Facilities (Airport, Government, etc.) - Check the box if some special facility lost telecommunication service.

Other (please specify) – Fill in any other services affected.

Number of Potentially Affected

Blocked Calls – Provide the number of blocked calls. If no calls were blocked, please leave the field blank or put 0 down. If blocked call information is available in only one direction for interoffice facilities which handle traffic in both directions, the total number of blocked calls shall be estimated as twice the number of blocked calls determined for the available direction.

If real time information is not available, providers may provide data for the same day(s) of the week and the same time(s) of day as the outage, covering a time interval not older than 90 days preceding the onset of the outage in an effort to estimate blocked calls. In this case, the number of blocked calls reported should be 3 times the historic carried load.

If, for whatever reason, real-time and historic carried call load data are unavailable to the provider, even after a detailed investigation, the provider must estimate the carried call load based on data obtained in the time interval between the repair of the outage and the due date for the Final Report; this data must cover the same day of the week, the same time of day, and the same duration as the outage. Justification that such data accurately estimates the traffic that would have been carried at the time of the outage must be available on request. In this case, the estimate of the number of blocked calls reported should be 3 times carried load. The number of blocked calls, if known, must be filled out even if it is not the trigger for an outage being reportable.

Real-Time, Historic Check Box - Check off whether the number of blocked calls came from real-time data or was based on historic carried loads the same day(s) of the week and the same time(s) of day as the outage.

DS3s – Provide the number of previously operating DS3s that were affected by the outage regardless of the services carried on the DS3s or the utilization of the DS3s. If service is provided over an OC3c or OC12c assume that all of the capacity was working and report 3 DS3s for an OC3c or 12 DS3s for an OC12c, etc..

Lost SS7 MTP Messages - In cases of an SS7 outage and where an SS7 provider cannot directly estimate the number of blocked calls, provide the number of real-time lost SS7 MTP messages or the number SS7 MTP messages carried on a historical basis. Historic carried SS7 MTP messages should be for the same day(s) of the week and the same time(s) of day as the outage. The information should not be older than 90 days preceding the onset of the outage. If the outage does not affect an SS7 network, please leave this field blank.

Geographic Area Affected

State – Choose the (primary) state from the scroll down menu affected by the outage. All 50 states along with the District of Columbia and Puerto Rico are listed. In addition outages affecting major parts of more than one state should be listed as multi-state. Finally, if an outage occurred outside the fifty states, the District of Columbia, or Puerto Rico, please choose “Outside the 50 States”.

City – Provide the (primary) city affected.

More Complete Description of Geographical Area of Outage – Provide a more complete description of the geographical area of the outage. In particular, for the cases affecting widespread outages in several states, it is important to list the states affected. For outages affecting more than one community, it is important to describe actual communities affected. Include CLLIs if applicable.

Description of Incident - Provide a narrative which describes the sequence of events leading up to the incident, the steps taken to try and resolve the incident once it had occurred, and the action(s) which finally brought resolution to the incident. This is for the reader to better understand what has happened. Include any factors which may have contributed to the duration of the incident, "quick fix" actions which may have resolved the immediate problem but were not the final, long-term solution, and any other contributing factors. The description should be sufficiently detailed to allow the reader to reach the same conclusions as the writer as to the Direct Cause and Root Cause of the incident.

Description of the Cause(s) of the Outage – Provide a text description of all the causes of the outage. This text should be in the own words of the outage inputter and should not use the words in the pull-down menus for Direct Cause or Root Cause.

Direct Cause: The direct cause is the immediate event that results in an outage – Scroll down the menu and choose the direct cause that is the most accurate. The direct cause is the event, action, or procedure that triggered the outage. In the Appendix there is a complete description of each of the direct causes. For example, a cable cut improper marking could be the triggering event or direct cause but the real cause or root cause may be lack of diversity.

Root Cause: The root cause is the underlying reason why the outage occurred or why the outage was reportable. For example, a cable cut might not be reportable if all of the circuits in the cable were on working SONET rings, but would be reportable if both SS7 A-links for multiple wire centers were in the cable with no diversity. - Scroll down the menu and pick the root cause that best fits. Root Cause is the key problem which once identified and corrected will prevent the same or a similar problem from recurring. With today's technology, two or more problems may be closely linked and require detailed investigation. However, in any single incident there should be only one

primary cause - the Root Cause. In the Appendix there is a complete description of each root cause. For example, a cable cut improper marking could be the triggering event or direct cause but the real cause (root cause) may be lack of diversity.

Contributing Factors – Scroll down the menu and pick the contributing factors that best fit. Contributing factors are problems or causes that are closely linked to the outage. Often if a contributing factor were addressed beforehand, the outage could have been prevented or the effect of the outage would have been reduced or eliminated. The form allows two contributing factors.

Diversity Indicator – Determine whether lack of diversity contributed to or caused the outage. If Best Practices related to diversity are discussed in any of the Best Practice fields, or if the lack of diversity is listed as a root cause or contributing factor to the outage, then the diversity checkbox must also be checked. In general, determine whether engineering standards for diversity are being followed.

Malicious Activity – Indicate whether you believe that malicious activity might be involved in the outage. The form asks for some explanation of why you believe the activity is malicious or what is suspicious about the activity. Malicious activity could be the product of terrorists.

Name and Type of Equipment that Failed - Provide the vendor name and the specific equipment (including software release if applicable) involved in the outage. For example, if a relay in a power plant fails that subsequently causes a switch to go out of service due to lack of power, then report the make and model of the relay, not the power plant or switch.

Specific Part of the Network Involved – Provide the part of the network involved with the incident. Examples are local switch, tandem switch, signaling network, central office power plant, digital cross-connect system, outside plant cable, ALI database, etc.

Method(s) Used to Restore Service - Provide a complete, chronological narrative of the methods used to restore service, both "quick fix" and final.

Telecommunications Service Priority (TSP) Indicator – Indicate whether TSP was used during service restoration.

Steps Taken to Prevent Reoccurrence – Provide the steps already taken and to be taken to prevent reoccurrence. Typically the corrective actions are identified through a Root Cause Analysis of the incident and the steps for prevention can be at both this location and throughout the network(s) if appropriate. If a time frame for implementation exists it should be provided. If no further action is required or planned, the service provider should so indicate.

Applicable Best Practices that might have prevented the Outage or reduced its effects – Provide a description of the Best Practices that could have prevented the outage

or reduced its effects. The Network Reliability and Interoperability Council has developed a list of Best Practices. They can be accessed via www.nric.org. You can find relevant Best Practices by using keywords.

Best Practices used to diminish effects of Outage - Provide a description of the most important Best Practices that were actually used to lessen the effects of the outage. These chosen Best practices helped shorten the outage, reduced the restoration times, prevented the outage from affecting more customers, and/or reduced the effects on customers (ensured that E911 was not affected). If none were used, please leave blank.

Analysis of Best Practices – Provide an evaluation of the relevance, applicability and usefulness of the current Best Practices for the outage. If a new Best Practice is needed or an existing Best Practice needs to be modified, please indicate this.

Remarks – Provide any additional information that you believe is relevant but did not fit anywhere else on the form.

Primary Contact Person – Provide the full name of the primary contact person

Phone Number – Provide the phone number of the primary contact person in the format NXX-NXX-XXXX. That is, 201-444-5656 would mean that the area code or NPA is 201, the central office code is 444, and the line number is 5656.

Extension – Provide the extension number, if used, in format XXXX.

U.S. Postal Service Address – Provide the address of the primary contact person.

E-mail Address – Provide the e-mail address of the primary contact person.

Secondary Contact Person – Provide the full name of the secondary contact person.

Phone Number – Provide the phone number of the secondary contact person in the format NXX-NXX-XXXX. That is, 201-444-5656 would mean that the area code or NPA is 201, the central office code is 444, and the line number is 5656.

Extension – Provide the extension number, if used, in format XXXX.

U.S. Postal Service Address – Provide the address of the secondary contact person.

E-mail Address – Provide the e-mail address of the secondary contact person.

4 Descriptions of Root Cause, Direct Cause and Contributing Factors

Cable Damage

Cable unlocated

This is considered a procedural error. Prior notification of action was provided by the excavator but the facility owner or locating company failed to establish the presence of a cable which was then eventually damaged.

Digging error

Excavator error during digging (contractor provided accurate notification, route was accurately located and marked, and cable was buried at a proper depth with sufficient clearance from other sub-surface structures).

Inadequate/no notification

Excavator failed to provide any notification prior to digging, or did not accurately describe the location of the digging work to be performed.

Inaccurate cable locate

This is considered a procedural error. The cable's presence was determined, but its location was inaccurately identified.

Shallow cable

The cable was at too shallow a depth, (notification was adequate, locate was accurate, excavator followed standard procedures).

Other

Design - Firmware

Ineffective fault recovery or re-initialization action

Failure to reset/restore following general/system restoral/initialization.

Insufficient software state indications

Failure to communicate or display out-of-service firmware states; failure to identify, communicate or display indolent or "sleepy" firmware states.

Other

Design - Hardware

Inadequate grounding strategy

Insufficient component grounding design; duplex components/systems sharing common power feeds/fusing.

Poor backplane or pin arrangement

Non-standard/confusing pin arrangements or pin numbering schemes; insufficient room or clearance between pins; backplane/pin crowding.

Poor card/frame mechanisms (latches, slots, jacks, etc.)

Mechanical/physical design problems.

Other

Design – Software

Faulty software load - office data

Inaccurate/mismatched office configuration data used/applied; wrong/defective office load supplied

Faulty software load - program data

Bad program code/instructions; logical errors/incompatibility between features/sets; software quality control failure; wrong/defective program load supplied.

Inadequate defensive checks

Changes to critical or protected memory were allowed without system challenge; contradictory or ambiguous system input commands were interpreted/responded to without system challenge. Failure of system to recognize or communicate query/warning in response to commands with obvious major system/network impact.

Ineffective fault recovery or re-initialization action

Simple, single-point failure resulting in total system outage; failure of system diagnostics resulting from the removal of a good unit with restoral of faulty mate; failure to switch/protect the switch to standby/spare/mate component(s).

Other

Diversity Failure

External

Failure to provide or maintain the diversity of links or circuits among external network components which results in a single-point-of-failure configuration.

Links

SS7 communication paths were not physically and logically diverse.

Power

Failure to diversify links, circuits, or equipment among redundant power system components, including ac rectifiers/chargers, battery power plants, dc distribution facilities, etc.

Timing Equipment

Failure to diversify critical equipment across timing supplies (e.g., BITS clocks)

Internal (Other)

Failure to provide or maintain diversity of equipment internal to a building. This is excluding power equipment and timing equipment.

Environment – External (for limited use when applicable root causes caused by a service provider or vendor cannot be identified; it can also be listed as contributing factor)

Earthquake

Component destruction or fault associated directly or indirectly with seismic shock. However, if damage was the result of inadequate earthquake bracing, consider the fault to be a hardware design.

Fire

Component destruction or fault associated with a fire occurring/starting outside the service provider plant. This includes brush fires, pole fires, etc.

Lightning/transient voltage

Component destruction or fault associated with surges and over-voltages caused by (electrical) atmospheric disturbances.

Storm - water/ice

Component destruction or fault associated with fog, rain, hail, sleet, snow, or the accumulation of water/ice (flooding, collapse under weight of snow, etc.).

Storm - wind/trees

Component destruction or fault associated with wind-borne debris or falling

trees/limbs.

Vandalism/theft

Component loss, destruction, or fault associated with larceny, mischief, or other malicious acts.

Vehicular accident

Component destruction or fault associated with vehicle (car, truck, train, etc.) collision.

Other

Environment (Internal)

Cable pressurization failure

Component destruction or fault associated with cable damage resulting from cable pressurization failure.

Dirt, dust contamination

Component loss or fault associated with dirt or dust, typically resulting in component overheating, or loss of connectivity.

Environmental system failure (heat/humidity)

Component loss or fault associated with extreme temperature, rapid temperature changes, or high humidity due to loss/malfunction of environmental control(s). If the failure was the result of inadequate/lack of response to (alarmed/un-alarmed) environmental failures, or due to incorrect manual control of environmental systems, consider this a procedural fault.

Fire, arcing, smoke damage

Component loss or fault associated with damage directly related to central office or equipment fires (open flame or smoldering), corrosive smoke emissions, or electrical arcing (whether or not ignition of surrounding material occurs).

Fire suppression (water, chemicals) damage

Component loss or fault associated with corrosion (electrolytic or other) caused by fire suppression activities; this root cause assumes that no substantial failure was directly associated with the smoke/fire that triggered suppression.

Manhole/cable vault leak

Component destruction or fault associated with water entering manholes, cable vaults, CEVs, etc.

Roof/air conditioning leak

Component destruction or fault associated with water damage (direct or electrolytic) caused by roof or environmental systems leaks into/in central office environment.

Other

Hardware Failure

Memory unit failure

Peripheral unit failure

Processor community failure

Other

Insufficient Data

There is not enough information from the failure report (and subsequent

investigation, if any) to determine cause(s) of failure.

Other/Unknown

The cause of the outage cannot be determined, or the cause does not match any of the classifications above. Excludes cases where outage data was insufficient or missing, or where root cause is still under investigation. When root cause cannot be proven, it is usually still possible to determine the probable cause, which falls under the heading "unknown." When classifications provided do not match the cause, the approximate match is preferred to be "other."

Power Failure (Commercial and/or Back-up) (does not include failures of dc/dc converters or fuses embedded in switches and transmission equipment, which should be reported as a hardware failure, unless the problem was caused by the power plant.)

Battery Failure

Batteries did not function as designed.

Extended Commercial Power Failure

System failure due to commercial power failure that extends beyond the design of back-up capabilities

Generator Failure

Generator did not function as designed or ran out of fuel.

Inadequate/missing power alarm

System failure associated to an un-alarmed (or under-alarmed) power failure, an alarm not provided initially due to inadequate standards, failure to implement standards or an alarm/alarm system failure (broken or modified).

Because of the success in avoiding severe, battery-depletion failure where power alarms are effective and effectively responded to, system failures directly associated with power alarms should be classified as such, instead of as procedural.

Inadequate site-specific power contingency plans

System failure due to the insufficiency of the emergency operating procedures and contingency plans available and the resulting outage is prolonged because of lack of site-specific information. This includes equipment engineering data, portable engine hook-up hardware/procedures, load shedding plans, etc.

Insufficient response to power alarm

System failure associated response to power failure: alarm system worked but support personnel did not respond properly. Consider this a procedural fault.

Lack of power redundancy

Failure directly associated with insufficient redundancy of power system components, including ac rectifiers/chargers, battery power plan, dc distribution facilities, etc

Lack of routine maintenance/testing

System failure resulting from infrequent power system testing, maintenance and/or detailed inspection. Consider this a procedural fault.

Overloaded/undersized power equipment

System failure attributable to insufficient sizing/design of power configuration
Other

Procedural - Other Vendor

Ad hoc activities, outside scope of MOP

Unapproved, unauthorized work, or changes in agreed-to procedures.

Documentation/procedures out-of-date, unusable, impractical

Lack of updated documentation/procedures, the correction/update is available but not incorporated locally, or the document is unwieldy. Some examples are the use of inadequate indexing or cross-referencing, bits and pieces of information being too difficult to integrate, ineffective delivery vehicle, etc.

Documentation/procedures unavailable, incomplete

Documentation or procedures (vendor or service provider) are not published; published, but not distributed; distributed, but not available on-site, or that some documentation is obscure/oblique, too general (lack of practical detail), too detailed/technical for practical use, etc.

Insufficient supervision/control

Resulting from insufficient leadership, ineffective administration, and/or maintenance strategies (process or communication failures; conflicting priorities) etc. This category should be used when multiple procedural causes are indicated.

Insufficient training

Training not available from vendor; training not available from service provider; training available but not attended; training attended but provides inadequate or out-of-date information; training adequate but insufficient application followed; training need never identified, etc.

Other

Procedural - Service Provider

Documentation/procedures out-of-date unusable or impractical

Documentation/procedures are not updated; correction/update available but not incorporated locally. Documentation/procedures are unwieldy; inadequate indexing or cross-referencing; bits and pieces of information difficult to integrate; ineffective delivery vehicle, etc.

Documentation/procedures unavailable/unclear/incomplete

Documentation or procedures (vendor or service provider) are not published; published, but not distributed; distributed, but not available on-site, etc. Documentation/procedures are obscure/oblique; too general - insufficient specificity; too detailed/technical for practical use, etc.

Inadequate routine maintenance/memory back-up

Failure could have been prevented/minimized by simple maintenance routines. The resulting recovery action was delayed/complicated by old or missing program/office data tapes or disks, etc.

Insufficient staffing

Unexpected conditions depleted available resources; predictable but unavoidable shortage (unreasonable demand); ineffective/inadequate roll-down or

centralization arrangement; resource-intensive (new) technology outside scope/reach of existing automatic/remote administration systems, etc.

Insufficient supervision/control

Resulting from insufficient leadership, ineffective administration, and/or maintenance strategies (process or communication failures; conflicting priorities) etc. This category should be used when multiple procedural causes are indicated.

Insufficient training

Training not available from vendor; training not available from service provider; training available but not attended; training attended but provides inadequate or out-of-date information; training adequate but insufficient application followed; training need never identified, etc

Other

Procedural - System Vendor

Ad hoc activities, outside scope of MOP

Unapproved, unauthorized work or changes in agreed-to procedures.

Documentation/procedures out-of-date unusable or impractical

Documentation/procedures are not updated; correction/update available but not incorporated locally. Documentation/procedures are unwieldy; inadequate indexing or cross-referencing; bits and pieces of information difficult to integrate; ineffective delivery vehicle, etc.

Documentation/procedures unavailable/unclear/incomplete

Documentation or procedures (vendor or service provider) are not published; published, but not distributed; distributed, but not available on-site, etc. Documentation/procedures are obscure/oblique; too general - insufficient specificity; too detailed/technical for practical use, etc.

Insufficient staffing

Unexpected conditions depleted available resources; predictable but unavoidable shortage (unreasonable demand); ineffective/inadequate roll-down or centralization arrangement; resource-intensive (new) technology outside scope/reach of existing automatic/remote administration systems, etc.

Insufficient supervision/control

Resulting from insufficient leadership, ineffective administration, and/or maintenance strategies (process or communication failures; conflicting priorities) etc. This category should be used when multiple procedural causes are indicated.

Insufficient training

Training not available from vendor; training not available from service provider; training available but not attended; training attended but provides inadequate or out-of-date information; training adequate but insufficient application followed; training need never identified, etc.

Other

Simplex Condition

Non-service affecting

Occurs when there is a failure of one side of a duplexed system such as a SONET

ring yet an unprotected simplex service will still provide service for the duration of the outage. Do not use this root cause for the complete failure of a duplexed system or in cases where any of the circuits in the duplexed system are provided under SLAs which require protection.

Service affecting

Failure of one side of a duplexed system such as a SONET ring where an unprotected simplex service was provided for a period of time but was not repaired during the usual maintenance window or in cases where any of the circuits in the duplexed system are provided under SLAs which require protection.

Traffic/System Overload

Common channel signaling network overload

SS7 system/network overload associated with (true) high traffic loads congesting STP/SCP processors or SS7 link network. If the overload was associated with STP/SCP message handling congestion, false or reactivated link congestion, inappropriate or incorrect SS7 network management message(s), protocol errors, etc., then consider the problem to be a software design fault.

Inappropriate/insufficient NM control(s)

System/network overload or congestion associated with an ineffective NM system/switch response resulting due to the lack of either effective NM control, that the system/switch response to control was inappropriate, or that its implementation was flawed. If failure was related to inappropriate control strategy or execution by NM organization, consider it procedural.

Ineffective engineering/engineering tools

System/network overload or congestion directly associated with under-engineering of the system/network due to rapidly changing network demand, or introduction of new network components and/or technologies. If failure was associated with simple under-engineering (absent changing environment), consider it procedural.

Mass calling - focused/diffuse network overload

System/network overload or congestion directly associated with unplanned, external trigger(s) causing a significant, unmanageable traffic load.

Media-stimulated calling - insufficient notification

System/network overload or congestion directly associated with a media-stimulated calling event where the event sponsor/generator failed to provide adequate advance notice, or provided inaccurate (underestimated) notification.

Other